REMARKS

I. Introductory Remarks

This is a full response to the outstanding final Office Action mailed July 30, 2007. Through this response claims 12–13, 15 and 21–29 have been amended. Claims 1–11 have been previously withdrawn. Claims 30–37 are newly added. Claims 12–37 are pending in the present Application. In view of the following remarks, reconsideration and allowance of the Application and presently pending claims are respectfully requested.

II. Summary

In an effort to further clarify the goals of the present invention, a brief overview is presented. The present invention provides a random number to be used in a computer program application that requires the random number for secure electronic communications. A digital signature is provided for a received message, and then is provided as the random number for the computer program application. Examples of computer program applications that use random numbers in secure electronic communications are security protocols as recited in the application at *page 17, lines 20–24*:

> Random numbers are utilized in may [sic, many] computer applications, such as in security protocols like secure socket layer (SSL) protocol and pretty good privacy (PGP) for the creation of session keys. Yet another feature of the present invention includes the generation of a digital signature using a digital signature algorithm, with the resulting digital signature being used in such an application as a random number.

The present inventions thus provide for the use of a digital signature as a random number in the creation of a session key for a SSL protocol as recited in the application at *page 92, lines 11–18*:

> In such protocol, it is customary for the computer 3202 to generate a random number for use in creating a session key for the SSL communication. In accordance with a further feature of the present invention, the IC card 95 is used for the provision of the random number for creation of the session key. In particular, a digital signature is originated by the IC card 95 and used as the random number itself for the purpose of creating the session key. An indirect

> result of the DSA and ECDSA specified in FIPS PUB 186-2 is that the resulting digital signature itself is a random number.

Thus, a digital signature for a received message is provided for use as a random number in computer applications that require random numbers for secure electronic communications, but the digital signature may also be used as a random number for the generation of another digital signature.

III. Response to Action Made Final

Applicants respectfully submit the present response should not have been made final. Applicants note that the MPEP § 706.07(a) allows that "[w]here information is submitted in a reply to a requirement under 37 CFR 1.105, the examiner may NOT make the next Office action relying on that art final unless all instance of the application of such art are necessitated by amendment." However, while there was no formal 37 CFR 1.105 requirement, in the Office Action dated July 14, 2005, the Examiner noted that the "exorbitant amount of prior art … do not all appear to have relevancy or pertinence to the" invention as claimed, and specifically requested that Applicants "point out which of these numerous prior art are pertinent or relevant to the patentability of the invention as claimed." Applicants responded with the requested suggestions as to the most relevant art submitted, in the Amendment filed January 2, 2007.

While the Examiner's request was not issued as a formal requirement under 37 C.F.R. § 1.105, the request nevertheless intimated, possibly, a less than thorough review of the submitted materials. Applicants respectfully note that the request could be seen as an informal request, but an informal request that differs only in name from a formal requirement.

That the section in the MPEP allows or requires, dependent upon interpretation, an Office Action to be made final, does not necessarily mean that is the best way to handle the circumstance. If the goal truly is to move the application forward, and to determine whether an application is patentable, then Applicants respectfully submit that the request should have been treated as a *de facto* requirement and that, as such, the Office Action should have been non-final.

IV. Response to Rejection of Claims 12, 15–17, 21, and 24–26 Under 35 U.S.C. § 102(b)

A. Statement of the Rejection

Claims 12, 15–17, 21, and 24–26 have been rejected under 35 U.S.C. § 102(b) as allegedly anticipated by U.S. Patent No. 5,422,953 to Fischer, hereinafter referenced as *Fischer*. Applicants respectfully traverse this rejection. Applicants have amended independent claims 12 and 21, to better indicate providing the generated digital signature to a computer program application such that the digital signature constitutes a random number for use by the computer program application for secure electronic communications. Thus, the discussion below addresses the Office Action arguments in the context of the amended independent claims 12 and 21.

B. Discussion of the Rejection

For a proper rejection of a claim under 35 U.S.C. § 102(b), the cited reference must disclose all elements, features and steps of the claim. *See, e.g., E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 7 U.S.P.Q.2d 1129(Fed. Cir. 1988) (Emphasis added). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(b). In the present case, not every feature of the claims is present in the *Fischer* reference.

1. Independent Claim 12

Applicants have amended independent claim 12 to more clearly indicate providing the generated digital signature to a computer program application such that the digital signature constitutes a random number for use by the computer program application for secure electronic communications. Independent claim 12, as amended recites:

12. A method for providing a random number for utilization in ~~an~~ a computer program application that requires the random number for secure electronic communications, the method comprising the steps of:
creating a private key of a public/private key pair within a secure device;
upon receipt of message data at the secure device, originating a digital signature for the message data, the originating comprising:
calculating a hash value for the message data;
encrypting at least the hash value using the private key; and
providing results of the encrypting step as a generated digital signature; and
providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

(Emphasis added.)

Independent claim 12 is allowable over *Fischer* for at least the reason that *Fischer* does not teach the features that are highlighted in independent claim 12 above. More specifically, *Fischer* does not teach "providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications," as recited in the amended independent claim 12.

Fischer appears to teach the combining of "digital time notarization into a digital signature operation to ensure that a time stamp is always automatically present." *Fischer, Abstract.* Thus, *Fischer* appears to be concerned with validating the timing of a digital signature rather than with the digital signature and its uses. Specifically, *Fischer* recites allowing "an automatic trusted time stamp to be incorporated into user's digital signature operation so that no additional user steps are necessary." *Fischer, column 2, lines 6–9.* However, there is no mention of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

Adding a time stamp to a digital signature is not the same as providing the newly generated digital signature to an external computer program application for use as a random number by the computer program application for secure electronic communications. Thus,

Applicants respectfully submit that *Fischer* does not teach "providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications," as recited in the amended independent claim 12.

Applicants respectfully submit that since *Fischer* does not anticipate independent claim 12, as amended, claim 12 is in condition for allowance and the rejection should be withdrawn. Further, Applicants respectfully submit that because independent claim 12 is allowable, as argued above, dependent claims 15–17, and indeed the remaining dependent claims 13–14 and 18–20, are allowable as a matter of law for at least the reason that they contain all the elements, features and limitations of independent claim 12. *See In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988). Therefore, Applicants respectfully request that the rejection of these claims be withdrawn.

2. Independent Claim 21

Applicants have amended independent claim 21 to more clearly indicate providing the generated digital signature to a computer program application such that the digital signature constitutes a random number for use by the computer program application for secure electronic communications. Independent claim 21, as amended recites:

> 21. A secure device for providing a random number for utilization within a computer program application that requires the random number for secure electronic communications, the secure device comprising:
> a user interface for receipt of message data;
> a memory means for the storage of a private key of a public/private key pair;
> a digital signature component in communication with the memory means,
> wherein the digital signature component originates a digital signature for the message data, the origination comprising:
> calculation of a hash value for the message data;
> encryption of at least the hash value using the private key; and
> provision of the encryption results as a generated digital signature; and
> ***an output means for providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by***

the computer program application for secure electronic communications.

(Emphasis added.)

Independent claim 21 is allowable over *Fischer* for at least the reason that *Fischer* does not teach the features that are highlighted in independent claim 21 above. More specifically, *Fischer* does not teach "an output means for providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications," as recited in independent claim 21.

As argued above, *Fischer* appears to teach the combining of "digital time notarization into a digital signature operation to ensure that a time stamp is always automatically present." *Fischer, Abstract.* Thus, *Fischer* appears to be concerned with validating the timing of a digital signature rather than with the digital signature and its uses. Specifically, *Fischer* recites allowing "an automatic trusted time stamp to be incorporated into user's digital signature operation so that no additional user steps are necessary." *Fischer, column 2, lines 6–9.* However, there is no mention of an output means for providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

Adding a time stamp to a digital signature is not the same as providing the generated digital signature to an external computer program application for use as a random number by the computer program application for secure electronic communications. Thus, Applicants respectfully submit that *Fischer* does not teach "an output means for providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications," as recited in the amended independent claim 21.

Applicants respectfully submit that since *Fischer* does not anticipate independent claim 21, as amended, independent claim 21 is in condition for allowance and the rejection should be withdrawn. Further, Applicants respectfully submit that because independent claim 21 is allowable, as argued above, dependent claims 24–26, and indeed the remaining dependent claims 22–23 and 27–29, are allowable as a matter of law for at least the reason that they contain all the elements, features and limitations of amended independent claim 21. *See In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988). Therefore, Applicants respectfully request that the rejection of these claims be withdrawn.

V. Response to Rejection of Claims 13, 14, 18–20, 22, 23, and 27–29 Under 35 U.S.C. § 103(a)

A. Statement of the Rejections

Claims 13 and 22 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fischer*, in view of U.S. Patent No. 6,775,772 to Binding *et al.*, hereinafter referenced as *Binding*. Claims 14 and 23 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fischer*, in view of U.S. Patent No. 6,073,237 to Ellison, hereinafter referenced as *Ellison*. Claims 18 and 27 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fischer*, and further in view of Applicants' Admitted Prior Art hereinafter referenced as *AAPA*. Claims 19–20 and 28–29 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fischer*, in view of *AAPA*, and further in view of U.S. Patent No. 6,594,759 to Wang, hereinafter referenced as *Wang*.

Applicants respectfully traverse these rejections. Applicants have amended independent claims 12 and 21, to better indicate providing the generated digital signature to a computer program application such that the digital signature constitutes a random number for use by the computer program application for secure electronic communications. Thus, the discussion below addresses the Office Action arguments in the context of the amended independent claims 12 and 21.

B. Discussion of the Rejections

Before specifically discussing the reasons for nonobviousness, we will briefly review the state of the law under the recent Supreme Court case of *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 127 S.Ct. 1727 (2007).

The United States Patent and Trademark Office (USPTO) has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness according to the factual inquiries expressed in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), namely: (1) determine the scope and content of the prior art, (2) ascertain the differences, if any, between the claimed subject matter and the prior art, (3) determine the level of skill in the pertinent art. Against this background, determination must be made as to whether a person of ordinary skill in the relevant art would find the claimed invention obvious. Also, the Examiner should evaluate the effect of any secondary considerations of nonobviousness such as commercial success, long-felt but unsolved needs, failure of others, and unexpected results.

Applicants respectfully submit that a *prima facie* case of obviousness has not been established according to the art of record.

1. Dependent Claims 13 and 22

Applicants respectfully submit that *Fischer* in view of *Binding* does not teach the emphasized features as highlighted in independent claims 12 and 21. As argued above, adding a time stamp to a digital signature is not the same as providing the newly generated digital signature to an external computer program application for use as a random number by the computer program application for secure electronic communications.

Further, it is acknowledged in the Office Action that *Fischer* does not explicitly disclose the use of the digital signature as a safeguard against a replay attack. *Office Action, page 4.* Neither does *Binding* remedy the above deficiencies.

It is asserted in the Office Action that *Binding* teaches the use of the digital signature on a nonce as a safeguard against a replay attack *Office Action, p. 4.* Applicants respectfully disagree with this characterization of the *Binding* reference.

Binding appears to teach generation of a nonce, *i.e.*, a value created by a random number generator, to authenticate the identity of the other party. *Binding*, *column 9, line 64–column 10, line 11*. However, there is no mention of providing a generated digital signature for use as the random number used in generating a nonce or for use in any other application.

Applicants respectfully submit that the combination of *Fischer* and *Binding* does not provide any information, motivation, or teaching as regards the aspects of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

There is no combining of prior art elements according to known methods to yield a predictable result. As argued above, the combination of *Fischer* and *Binding* does not teach providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications. Even if *Binding* teaches the use of a digital signature as a safeguard against a replay attack, the functionality of the present invention is different than that of *Fischer*, *Binding*, or the combination of both. It would not be predictable to combine *Fischer* and *Binding* to produce the inventions as described in the present application, and indeed, the combination would not produce the desired result.

It should be apparent that there is no teaching, suggestion, or motivation in the prior art of *Fischer* or *Binding* that would have led one of ordinary skill to modify the reference or to combine prior art reference teachings to arrive at the claimed invention. Neither the use of a an automatic trusted time stamp in *Fischer* nor the use of a digital signature as a safeguard against a replay attack by *Binding* provide any applicable teaching, suggestion, or motivation of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications, as in independent claims 12 and 21. Even if *Binding* teaches the use of a digital signature as a safeguard against a replay attack, the present inventions do not result from the combination of *Fischer* and *Binding*, and there is no motivation to combine the references.

Applicants respectfully submit that the combination of *Fischer* and *Binding* does not teach, discuss, suggest, contemplate, or require the features of independent claims 12 and 21, as amended. Because independent claims 12 and 21 are allowable over the combination, dependent claims 13 and 22 are allowable as a matter of law for at least the reason that dependent claims 13 and 22 contain all elements, features and limitations of independent claims 12 and 21. *See*, *e.g.*, *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

In summary, it is Applicants' position that a case for obviousness has not been made against Applicants' claims 13 and 22. Therefore, it is respectfully submitted that each of these claims is patentable over *Fischer* in view *Binding*, and that the rejection of these claims should be withdrawn.

2. Dependent Claims 14 and 23

Applicants respectfully submit that *Fischer* in view of *Ellison* does not teach the emphasized features as highlighted in independent claims 12 and 21. As argued above, adding a time stamp to a digital signature is not the same as providing the newly generated digital signature to an external computer program application for use as a random number by the computer program application for secure electronic communications.

Further, it is acknowledged in the Office Action that *Fischer* fails to disclose generating a session key based on the digital signature. *Office Action, page 4.* Neither does *Ellison* remedy the above deficiencies.

It is asserted in the Office Action that *Ellison* teaches the generation of a session key based on a digital signature. *Office Action, p. 4.*

Ellison appears to teach securing data in a tamper resistant fashion on a computer connected to a network. *Ellison, Abstract.* However, there is no mention of providing the generated digital signature for use as the random number.

Applicants respectfully submit that the combination of *Fischer* and *Ellison* does not provide any information, motivation, or teaching as regards the aspects of providing the generated digital signature to a computer program application external to the secure device such

that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

There is no combining of prior art elements according to known methods to yield a predictable result. As argued above, the combination of *Fischer* and *Ellison* does not teach providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications. Even if *Ellison* teaches generating a session key based on the digital signature, the functionality of the present invention is different than that of *Fischer*, *Ellison*, or the combination of both. It would not be predictable to combine *Fischer* and *Ellison* to produce the inventions as described in the present application, and indeed, the combination would not produce the desired result.

It should be apparent that there is no teaching, suggestion, or motivation in the prior art of *Fischer* or *Ellison* that would have led one of ordinary skill to modify the reference or to combine prior art reference teachings to arrive at the claimed invention. Neither the use of a an automatic trusted time stamp in *Fischer* nor the use of a digital signature for generation of a session key by *Ellison* provide any applicable teaching, suggestion, or motivation of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications, as in independent claims 12 and 21. Even if *Ellison* teaches the generation of a session key based on a digital signature, the present inventions do not result from the combination, and there is no motivation to combine the references.

Applicants respectfully submit that the combination of *Fischer* and *Binding* does not teach, discuss, suggest, contemplate, or require the features of independent claims 12 and 21, as amended. Because independent claims 12 and 21 are allowable over the combination, dependent claims 14 and 23 are allowable as a matter of law for at least the reason that dependent claims 14 and 23 contain all elements, features and limitations of independent claims 12 and 21. *See*, *e.g.*, *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

In summary, it is Applicants' position that a case for obviousness has not been made against Applicants' claims 14 and 23. Therefore, it is respectfully submitted that each of these claims is patentable over *Fischer* in view *Ellison*, and that the rejection of these claims should be withdrawn.

3. Dependent Claims 18 and 27

Applicants respectfully submit that *Fischer* in view of *Applicants' Admitted Prior Art (AAPA)* does not teach the emphasized features as highlighted in independent claims 12 and 21. As argued above, adding a time stamp to a digital signature is not the same as providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

Further, it is acknowledged in the Office Action that *Fischer* does not explicitly disclose the use of the an elliptical curve digital signature algorithm. *Office Action, page 4.* Neither does *Binding* remedy the above deficiencies.

It is asserted in the Office Action that *AAPA* teaches that an elliptical curve digital signature algorithm is a common way to generate a digital signature. *Office Action, p. 5.*

Whether an elliptical curve digital signature algorithm is a common way to generate a digital signature has no bearing on the combination.

Applicants respectfully submit that the combination of *Fischer* and *AAPA* does not provide any information, motivation, or teaching as regards the aspects of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

There is no combining of prior art elements according to known methods to yield a predictable result. As argued above, the combination of *Fischer* and *AAPA* does not teach providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by

the computer program application for secure electronic communications. Even if *AAPA* teaches the use of an elliptical curve digital signature algorithm to generate a digital signature, the functionality of the present invention is different than that of *Fischer*, *AAPA*, or the combination of both. It would not be predictable to combine *Fischer* and *AAPA* to produce the inventions as described in the present application, and indeed, the combination would not produce the desired result.

It should be apparent that there is no teaching, suggestion, or motivation in the prior art of *Fischer* or *AAPA* that would have led one of ordinary skill to modify the reference or to combine prior art reference teachings to arrive at the claimed invention. Neither the use of an automatic trusted time stamp in *Fischer* nor the use of an elliptical curve digital signature algorithm to generate a digital signature by *AAPA* provide any applicable teaching, suggestion, or motivation of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications, as in independent claims 12 and 21. Even if *AAPA* teaches the use of an elliptical curve digital signature algorithm to generate a digital signature, the present inventions do not result from the combination, and there is no motivation to combine the references.

Applicants respectfully submit that the combination of *Fischer* and *AAPA* does not teach, discuss, suggest, contemplate, or require the features of independent claims 12 and 21, as amended. Because independent claims 12 and 21 are allowable over the combination of *Fischer* and *AAPA*, dependent claims 18 and 27 are allowable as a matter of law for at least the reason that dependent claims 18 and 27 contain all elements, features and limitations of independent claims 12 and 21. *See, e.g., In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

In summary, it is Applicants' position that a case for obviousness has not been made against Applicants' claims 18 and 27. Therefore, it is respectfully submitted that each of these claims is patentable over *Fischer* in view *AAPA*, and that the rejection of these claims should be withdrawn.

4. Dependent Claims 19–20 and 28–29

Applicants respectfully submit that *Fischer* in view of *AAPA*, and further in view of *Wang* does not teach the emphasized features as highlighted in independent claims 12 and 21. As argued above, adding a time stamp to a digital signature, and using elliptical curve digital signature algorithm to generate a digital signature, is not the same as providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

Further, it is acknowledged in the Office Action that the combination of *Fischer* and *AAPA* does not explicitly disclose that the random number generator is inaccessible from outside the computer chip. *Office Action, page 6.* Neither does *Wang* remedy the above deficiencies.

It is asserted in the Office Action that *Wang* teaches that the random number generator can be used solely by a computer chip. *Office Action, p. 6.*

Wang appears to teach a computer configured to authenticate a user to an electronic transaction system. *Wang, Abstract.* Specifically, *Wang* recites that "the private key may be generated internally," and that "a random number generator … may be employed to provide a random seed number for generating the set of private key/public key." However, there is no mention of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

Applicants respectfully submit that the combination of *Fischer*, *AAPA* and *Wang* does not provide any information, motivation, or teaching as regards the aspects of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications.

There is no combining of prior art elements according to known methods to yield a predictable result. As argued above, the combination of *Fischer*, *AAPA* and *Wang* does not teach providing the generated digital signature to a computer program application external to the

secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications. Even if *Wang* teaches that the random number generator can be used solely by a computer chip, the functionality of the present invention is different than that of *Fischer*, *AAPA*, *Wang* or the combination of all. It would not be predictable to combine *Fischer*, *AAPA*, and *Wang* to produce the inventions as described in the present application, and indeed, the combination would not produce the desired result.

It should be apparent that there is no teaching, suggestion, or motivation in the prior art of *Fischer*, *AAPA*, or *Wang* that would have led one of ordinary skill to modify the reference or to combine prior art reference teachings to arrive at the claimed invention. Neither the use of a an automatic trusted time stamp in *Fischer*, the use of an elliptical curve digital signature algorithm to generate a digital signature by *AAPA*, nor a random number generator that can be used solely by a computer chip by *Wang* provide any applicable teaching, suggestion, or motivation of providing the generated digital signature to a computer program application external to the secure device such that the generated digital signature constitutes a random number for use by the computer program application for secure electronic communications, as in independent claims 12 and 21. Even if *Wang* teaches a random number generator that can be used solely by a computer chip, the present inventions do not result from the combination, and there is no motivation to combine the references.

Applicants respectfully submit that the combination of *Fischer*, *AAPA*, and *Wang* does not teach, discuss, suggest, contemplate, or require the features of independent claims 12 and 21, as amended. Because independent claims 12 and 21 are allowable over the combination, dependent claims 19–20 and 28–29 are allowable as a matter of law for at least the reason that dependent claims 19–20 and 28–29 contain all elements, features and limitations of independent claims 12 and 21. *See*, *e.g.*, *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

In summary, it is Applicants' position that a case for obviousness has not been made against Applicants' claims 19–20 and 28–29. Therefore, it is respectfully submitted that each of these claims is patentable over *Fischer* in view of *AAPA*, and further in view of *Wang*, and that the rejection of these claims should be withdrawn.

VI. New Claims

As identified above, claims 30–37 have been newly added through this Response. Applicants respectfully submit that these new claims describe an invention novel and unobvious in view of the prior art of record and, therefore, respectfully request that these claims be held allowable.

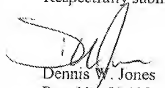
CONCLUSION

In light of the foregoing amendments and for at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the now pending claims 12–37, are in condition for allowance. Favorable consideration and allowance of the present Application and all pending claims are hereby courteously requested.

If, in the opinion of the Examiner, there are any issues that can be resolved by telephone conference, or if there are any informalities that may be addressed by an Examiner's amendment, the Examiner is invited to call the undersigned attorney at (404) 233-7000.

The Commissioner is hereby authorized to charge any fees due, or credit any overpayment, to Deposit Account No. **50-3537**.

Respectfully submitted,



January 11, 2008

Dennis W. Jones
Reg. No. 51,128

Morris, Manning and Martin, LLP
1600 Atlanta Financial Center
3343 Peachtree Road, N.E.
Atlanta Georgia 30326
404-233-7000 Main
404-365-9532 Facsimile
Our Docket No.: 10399-34383